Chapter 7

Wireless Applications

Introduction

Wireless Local Area Networks (LANs) allow mobile computers to communicate wirelessly and send captured data to a host device in real time. Before using the EDA on a WLAN, the facility must be set up with the required hardware to run the wireless LAN and the EDA must be configured. Refer to the documentation provided with the access points (APs) for instructions on setting up the hardware.

To configure the EDA, a set of wireless applications provide the tools to configure and test the wireless radio in the EDA. The *Wireless Application* menu on the task tray provides the following wireless applications:

- Wireless Status
- Wireless Diagnostics
- Find WLANs
- Manage Profiles
- Options
- Enable/Disable Radio
- Log On/Off.

Tap the *Signal Strength* icon to display the *Wireless Applications* menu.

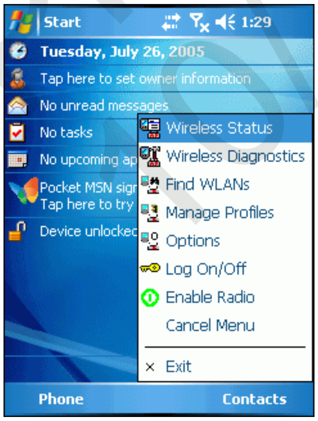


Figure 7-1 *Wireless Applications Menu*

Signal Strength Icon

The *Signal Strength* icon in the task tray indicates the EDA's wireless signal strength as follows:

Table 7-1 *Wireless Applications Icons, Signal Strength Descriptions*

Icon	Status	Action
	Excellent signal strength	Wireless LAN network is ready to use.
	Very good signal strength	Wireless LAN network is ready to use.
	Good signal strength	Wireless LAN network is ready to use.
	Fair signal strength	Wireless LAN network is ready to use. Notify the network administrator that the signal strength is only “Fair”.
	Poor signal strength	Wireless LAN network is ready to use. Performance may not be optimum. Notify the network administrator that the signal strength is “Poor”.
	Out-of-network range (not associated)	No wireless LAN network connection. Notify the network administrator.
	No wireless LAN network card detected	No wireless LAN network card detected or radio disabled. Notify the network administrator.

Turning the WLAN Radio On and Off

To turn the WLAN radio off tap the *Signal Strength* icon and select *Disable Radio*.

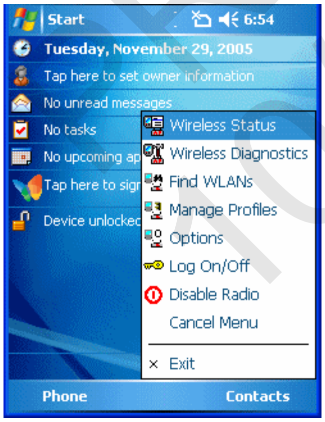


Figure 7-2 *Disable Radio*

To turn the WLAN radio on tap the *Signal Strength* icon and select *Enable Radio*.

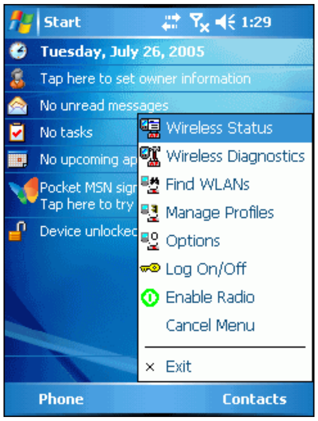
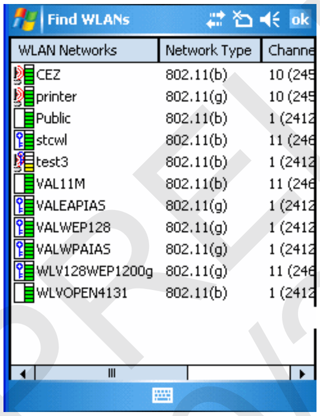


Figure 7-3 *Enable Radio*

Find WLANs Application

Use the *Find WLANs* application to discover available networks in the vicinity of the user and EDA. To open the *Find WLANs* application, tap the *Signal Strength* icon - *Find WLANs*. The *Find WLANs* window displays.



WLAN Networks	Network Type	Channe
CEZ	802.11(b)	10 (245
printer	802.11(g)	10 (245
Public	802.11(b)	1 (2412
stcwl	802.11(b)	11 (246
test3	802.11(b)	1 (2412
VAL11M	802.11(b)	11 (246
VALEAPIAS	802.11(g)	1 (2412
VALWEP128	802.11(g)	1 (2412
VALWPAIAS	802.11(g)	1 (2412
WLV128WEP1200g	802.11(g)	11 (246
WLVOPEN4131	802.11(b)	1 (2412

Figure 7-4 *Find WLANs Window*

✓ ***NOTE*** The *Find WLANs* display is limited to 32 items (ESSIDs or MAC addresses). A combination of up to 32 ESSIDs/APs may be displayed.

Manually enter valid ESSIDs not displayed in the *Find WLANs* window. See *Figure 7-5 on page 7-4*.

The *Find WLANs* list displays:

- WLAN Networks - Available wireless networks with icons that indicate signal strength and encryption type. The signal strength and encryption icons are described in Table 7-2 and Table 7-3.
- Network Type - Type of network.
- Channel - Channel on which the AP is transmitting.
- Signal Strength - The signal strength of the signal from the AP.

.

Table 7-2 *Signal Strength Icon*

Icon	Description
🟩	Excellent signal
🟩	Very good signal
🟨	Good signal
🟨	Fair signal
🟥	Poor signal
❗	Out of range or no signal

Table 7-3 *Encryption Icon*

Icon	Description
□	No encryption. WLAN is an infrastructure network.
📶	WLAN is an Ad-Hoc network.
🔑	WLAN access is encrypted and requires a password.

Tap-and-hold on a WLAN network to open a pop-up menu which provides two options: *Connect* and *Refresh*. Select *Refresh* to refresh the WLAN list. Select *Connect* to create a wireless profile from that network. This starts the *Profile Editor Wizard* which allows you to set the values for the selected network. After editing the profile, the EDA automatically connects to this new profile.

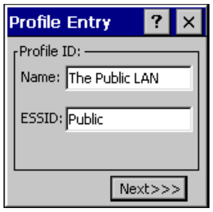
Profile Editor Wizard

Use the *Profile Editor Wizard* to create a new profile or edit an existing profile. If editing a profile, the fields reflect the current settings for that profile. If creating a new profile, the known information for that WLAN network appears in the fields.

Navigate through the wizard using the **Next** and **Back** buttons. Tap **X** to quit. On the confirmation dialog box, tap **No** to return to the wizard or tap **Yes** to quit and return to the *Manage Profiles* window. See *Manage Profiles Application on page 7-21* for instructions on navigating the *Profile Editor Wizard*.

Profile ID

In the *Profile ID* dialog box in the *Profile Editor Wizard*, enter the profile name and the ESSID.



Profile Entry

Profile ID:

Name: The Public LAN

ESSID: Public

Figure 7-5 *Profile ID Dialog Box*

Table 7-4 *Profile ID Fields*

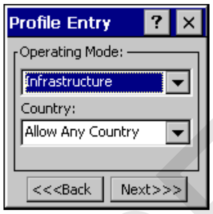
Field	Description
Name	The name and (WLAN) identifier of the network connection. Enter a user friendly name for the mobile computer profile used to connect to either an AP or another networked computer. Example: The Public LAN.
ESSID	The ESSID is the 802.11 extended service set identifier. The ESSID is 32-character (maximum) string identifying the WLAN, and must match the AP ESSID for the EDA to communicate with the AP.

✓ ***NOTE*** Two profiles with the same user friendly name are acceptable but not recommended.

Tap **Next.** The *Operating Mode* dialog box displays.

Operating Mode

Use the *Operating Mode* dialog box to select the operating mode (Infrastructure or Ad-Hoc) and the country location.



Operating Mode: Infrastructure

Country: Allow Any Country

Figure 7-6 *Operating Mode Dialog Box*

Table 7-5 *Operating Mode Fields*

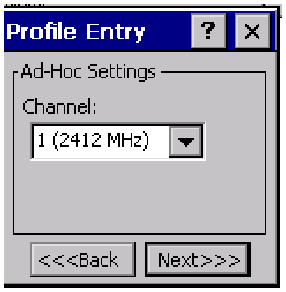
Field	Description
Operating Mode	Select *Infrastructure* to enable the EDA to transmit and receive data with an AP. Infrastructure is the default mode. Select *Ad Hoc* to enable the EDA to form its own local network where mobile computers communicate peer-to-peer without APs using a shared ESSID.
Country	*Country* determines if the profile is valid for the country of operation. The profile country must match the country in the options page or it must match the acquired country if 802.11d is enabled. **Single Country Use:** When the device is only used in a single country, set every profile country to *Allow Any Country*. In the *Options - Regulatory* dialog box (see *Figure 7-46 on page 7-35)*, select the specific country the device is used in, and deselect the *Enable 802.11d* option. This is the most common and efficient configuration, eliminating the initialization overhead associated with acquiring a country via 802.11d. **Multiple Country Use:** When the device is used in more than one country, select the *Enable 802.11d* option in the *Options - Regulatory* dialog box (see *Figure 7-46 on page 7-35)*. This eliminates the need for reprograming the country (in *Options - Regulatory*) each time you enter a new country. However, this only works if the infrastructure (i.e., APs) supports 802.11d (some infrastructures do not support 802.11d, including some Cisco APs). When the Enable 802.11d option is selected, the *Options - Regulatory - Country* setting is not used. For a single profile that can be used in multiple countries, with infrastructure that supports 802.11d (including Symbol infrastructure), set the Profile Country to *Allow Any Country*. Under *Options - Regulatory*, select *Enable 802.11d*. The *Options - Regulatory - Country* setting is not used. For a single profile that can be used in multiple countries, but with infrastructure that does not support 802.11d, set the profile country to *Allow Any Country*, and de-select (uncheck) *Enable 802.11d*. In this case, the *Options - Regulatory - Country* setting must always be set to the country the device is currently in. This configuration option is the most efficient and may be chosen for use with any infrastructure. However, the *Options - Regulatory - Country* setting must be manually changed when a new country is entered. Note that using a single profile in multiple countries implies that there is a common ESSID to connect to in each country. This is less likely than having unique ESSIDs in each country, this requires unique profiles for each country. For additional efficiency when using multiple profiles that can be used in multiple countries, the country setting for each profile can be set to a specific country. If the current country (found via 802.11d or set by *Options - Regulatory - Country* when 802.11d is disabled) does not match the country set in a given profile, then that profile is disabled. This can make profile roaming occur faster. For example, if two profiles are created and configured for Japan, and two more profiles are created and configured for USA, then when in Japan only the first two profiles are active, and when in USA only the last two are active. If they had all been configured for *Allow Any Country*, then all four would always be active, making profile roaming less efficient.

Tap **Next**. If *Ad-Hoc* mode was selected the *Ad-Hoc* dialog box displays. If *Infrastructure* mode was selected the *Authentication* dialog box displays. See *Authentication on page 7-7* for instruction on setting up authentication.

Ad-Hoc

Use the *Ad-Hoc* dialog box to select the required information to control *Ad-Hoc* mode. This dialog box does not appear if you selected *Infrastructure* mode. To select Ad-Hoc mode:

1. Select a channel number from the *Channel* drop-down list. The default is *Channel 1 (2412 MHz)*.



Channel: 1 (2412 MHz)

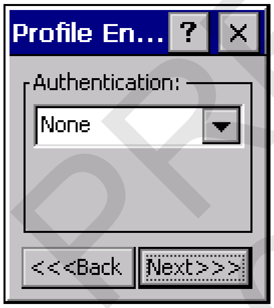
Figure 7-7 *Ad-Hoc Settings Dialog Box*

2. Tap **Next**. The *Authentication* dialog box displays.

Authentication

Use the *Authentication* dialog box to configure authentication. If you selected *Ad-Hoc* mode, this dialog box is not available and authentication is set to None by default.

Select an authentication type from the drop-down list and tap **Next**. Selecting *PEAP* or *TTLS* displays the *Tunneled* dialog box. Selecting *None*, *EAP TLS*, or *LEAP* displays the *Encryption* dialog box. See *Encryption on page 7-15* for encryption options. Table 7-6 lists the available authentication options.



Authentication: None

Figure 7-8 *Authentication Dialog Box*

Table 7-6 *Authentication Options*

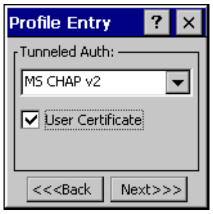
Authentication	Description
None	Default setting when authentication is not required on the network.
EAP TLS	Select this option to enable EAP TLS authentication. EAP TLS is an authentication scheme through IEEE 802.1x. It authenticates users and ensures only valid users can connect to the network. It also restricts unauthorized users from accessing transmitted information by using secure authentication certificates.

Table 7-6 *Authentication Options (Continued)*

Authentication	Description
PEAP	Select this option to enable PEAP authentication. This method uses a digital certificate to verify and authenticate a user's identity.
LEAP	Select this option to enable LEAP authentication, which is based on mutual authentication. The AP and the connecting mobile computer require authentication before gaining access to the network.
TTLS	Select this option to enable TTLS authentication.

Tunneled Authentication

Use the *Tunneled Authentication* dialog box to select the tunneled authentication options. There are different selections available for PEAP or TTLS authentication.



Tunneled Auth: MS CHAP v2

☑ User Certificate

Figure 7-9 *Tunneled Authentication Dialog Box*

To select a tunneled authentication type:

1. Select a tunneled authentication type from the drop-down list. See Table 7-7 and Table 7-8.
2. Select the *User Certificate* check box if a certificate is required. If you selected the TLS tunnel type that requires a user certificate, the check box is already selected.
3. Tap **Next**. The *Installed User Certificates* dialog box appears.

Table 7-7 lists the PEAP tunneled authentication options.

Table 7-7 *PEAP Tunneled Authentication Options*

PEAP Tunneled Authentication	Description
MS CHAP v2	Microsoft Challenge Handshake Authentication Protocol version 2 (MS CHAP v2) is a password-based, challenge-response, mutual authentication protocol that uses the industry-standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. MS CHAP v2 was originally designed by Microsoft as a PPP authentication protocol to provide better protection for dial-up and virtual private network (VPN) connections. With Windows XP SP1, Windows XP SP2, Windows Server 2003, and Windows 2000 SP4, MS CHAP v2 is also an EAP type.
TLS	EAP TLS is used during phase 2 of the authentication process. This method uses a user certificate to authenticate.

Table 7-8 lists the TTLS tunneled authentication options.

Table 7-8 *TTLS Tunneled Authentication Options*

TTLS Tunneled Authentication	Description
CHAP	Challenge Handshake Authentication Protocol (CHAP) is one of the two main authentication protocols used to verify the user name and password for PPP Internet connections. CHAP is more secure than PAP because it performs a three way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link is established.
MS CHAP	Microsoft Challenge Handshake Authentication Protocol (MS CHAP) is an implementation of the CHAP protocol that Microsoft created to authenticate remote Windows workstations. MS CHAP is identical to CHAP, except that MS CHAP is based on the encryption and hashing algorithms used by Windows networks, and the MS CHAP response to a challenge is in a format optimized for compatibility with Windows operating systems.
MS CHAP v2	MS CHAP v2 is a password based, challenge response, mutual authentication protocol that uses the industry standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. MS CHAP v2 was originally designed by Microsoft as a PPP authentication protocol to provide better protection for dial-up and virtual private network (VPN) connections. With Windows XP SP1, Windows XP SP2, Windows Server 2003, and Windows 2000 SP4, MS CHAP v2 is also an EAP type.
PAP	Password Authentication Protocol (PAP) has two variations: PAP and CHAP PAP. It verifies a user name and password for PPP Internet connections, but it is not as secure as CHAP, since it works only to establish the initial link. PAP is also more vulnerable to attack because it sends authentication packets throughout the network. Nevertheless, PAP is more commonly used than CHAP to log in to a remote host like an Internet service provider.
MD5	Message Digest-5 (MD5) is an authentication algorithm developed by RSA. MD5 generates a 128-bit message digest using a 128-bit key, IPSec truncates the message digest to 96 bits.

User Certificate Selection

If you checked the *User Certificate* check box on the *Tunneled Authentication* dialog box or if *TLS* is the selected authentication type, the *Installed User Certificates* dialog box displays. Select a certificate from the drop-down list of currently installed certificates before proceeding. The selected certificate's name appears in the drop-down list. If the required certificate is not in the list, install it.

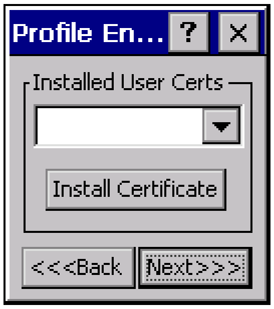
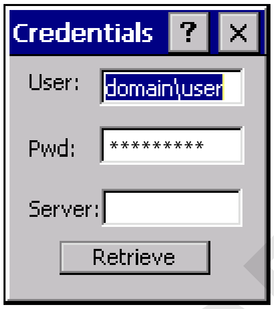


Figure 7-10 *Installed User Certificates Dialog Box*

User Certificate Installation

To install a user certificate (EAP TLS only) and a server certificate for EAP TLS and PEAP authentication:

1. Tap **Install Certificate**. The *Credentials* dialog box appears.



User: domain\user

Pwd: *********

Server:

Figure 7-11 *Credentials Dialog Box*

2. Enter the *User:*, *Pwd:* (password), and *Server:* information in their respective text boxes.
3. Tap **Retrieve**. A *Progress* dialog indicates the status of the certificate retrieval.
4. Tap **ok** to exit.

After the installation completes, the *Installed User Certs* dialog box displays.

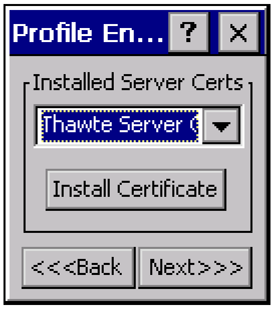
✓ ***NOTE*** To successfully install a user certificate, the EDA must already be connected to a network from which the server is accessible.

Server Certificate Selection

If you select the *Validate Server Certificate* check box, a server certificate is required. Select a certificate on the *Installed Server Certificates* dialog box. An hour glass may appear as the wizard populates the existing certificate list. If the required certificate is not listed, install it:

1. Select a certificate from the drop-down list of currently installed certificates.

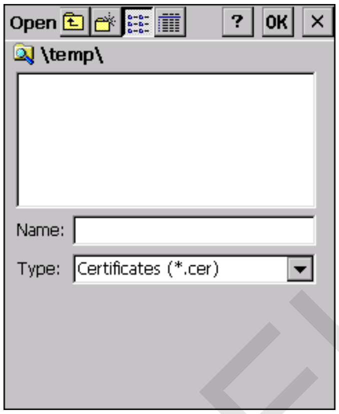
2. Tap the **Install Certificate** button.



Thawte Server C

Figure 7-12 *Installed Server Certificates Dialog Box*

A dialog lists the currently loaded certificate files found in the default directory (\Application\FusionApps\Certs) with the default extension.



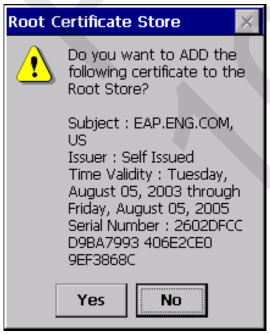
\temp\

Name:

Type: Certificates (*.cer)

Figure 7-13 *Browse Server Certificates*

Press the **ENT** key to change the default path or extension (and search a new path). Select a certificate before tapping the **Install** button.



Do you want to ADD the following certificate to the Root Store?

Subject : EAP.ENG.COM, US
Issuer : Self Issued
Time Validity : Tuesday, August 05, 2003 through Friday, August 05, 2005
Serial Number : 2602DFCC D9BA7993 406E2CE0 9EF3868C

Figure 7-14 *Confirmation Dialog Box*

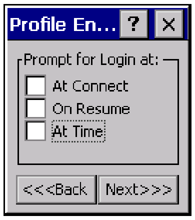
A confirmation dialog verifies the installation. If the information in this dialog is correct, tap the **Yes** button, If the information in this dialog is not correct tap the **No** button. The wizard returns to the *Installed Server Certs* dialog box.

Credential Cache Options

If you selected any of the password-based authentication types, you can select different credential caching options. These options specify when the network credential prompts appear: at connection, on each resume, or at a specified time.

Entering the credentials directly into the profile permanently caches the credentials. In this case, the EDA does not require user login. If a profile does not contain credentials entered through the configuration editor, you must log in to the EDA before connecting.

Caching options only apply on credentials entered through the login dialog box.



Prompt for Login at:

□ At Connect
□ On Resume
□ At Time

Figure 7-15 *Prompt for Login at Dialog Box*

If the EDA does not have the credentials, you are prompted to enter a username and password. If the EDA has the credentials (previous entered via a login dialog box), it uses these credentials unless the caching options require the EDA to prompt for new credentials. If you entered the credentials via the profile, the EDA does not prompt for new credentials. Table 7-9 lists the caching options.

Table 7-9 *Cache Options*

	Description
At Connect	Select this option to prompt for credentials whenever the WCS tries to connect to a new profile. Deselect this to use the cached credentials to authenticate. If the credentials are not cached, you are prompted to enter credentials. This option only applies when logged in.
On Resume	Selecting this reauthenticates an authenticated user when a suspend/resume occurs. Once reauthenticated, the user is prompted for credentials. If the user does not enter the same credentials that were entered prior to the suspend/resume within three attempts, the user is disconnected from the network. This option only applies when logged in.
At Time	Select this option to perform a local verification on an authenticated user at a specified time. The time can be an absolute time or a relative time from the authentication, and should be in at least 5 minute intervals. Once the time has passed, the user is prompted for credentials. If the user does not enter the correct credentials within three attempts, the user is disconnected from the network. This option only applies when logged in.

Entering credentials applies these credentials to a particular profile. Logging out clears all cached credentials. Editing a profile clears all cached credentials for that profile.

The following authentication types have credential caching:

- EAP TLS
- PEAP
- LEAP
- TTLS.

Selecting the *At Time* check box displays the *TIme Cache Options* dialog box.

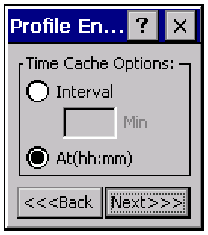


Figure 7-16 *Time Cache Options Dialog Box*

1. Tap the *Interval* radio button to check credentials at a set time interval.
2. Enter the value in minutes in the *Min* box.
3. Tap the *At (hh:mm)* radio button to check credentials at a set time.
4. Tap **Next**. The *At Time* dialog box appears.

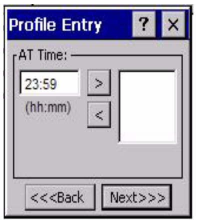


Figure 7-17 *At Time Dialog Box*

5. Enter the time using the 24 hour clock format in the *(hh:mm)* box.
6. Tap **>** to move the time to the right. Repeat for additional time periods.
7. Tap **Next**. The *User Name* dialog box displays.

The user name and password can be entered (but is not required) when the profile is created. When a profile authenticates with credentials that were entered in the profile, caching rules do not apply. Caching rules only apply on credentials that are entered through the login dialog box.

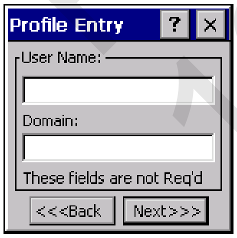


Figure 7-18 *Username Dialog Box*

Password

Use the *Password* dialog box to enter a password. If EAP/TLS is the selected authentication type, the password is not required and the field is disabled.

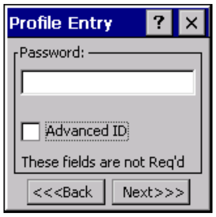


Figure 7-19 *Password Dialog Box*

1. Enter a password in the *Password* field.
2. Select the *Advanced ID* check box, if advanced identification is required.
3. Tap **Next.** The *Encryption* dialog box displays. See *Encryption on page 7-15*.

Advanced Identity

Use the *Advanced ID* dialog box to enter the 802.1X identity to supply to the authenticator. This value can be 63 characters long and is case sensitive. In TTLS and PEAP, it is recommended entering the identity *anonymous* (rather than a true identity) plus any desired realm (e.g., anonymous@myrealm). A user ID is required before proceeding.

✓ ***NOTE*** When authenticating with a Microsoft IAS server, do not use advanced identity.

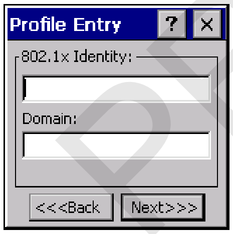
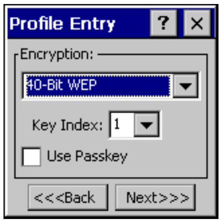


Figure 7-20 *Advanced Identity Dialog Box*

Tap **Next**. The E*ncryption* dialog box displays.

Encryption

Use the *Encryption* dialog box to select an encryption type. The drop-down list includes encryption types available for the selected authentication type. See Table 7-11 for these encryption types.



Encryption:

40-Bit WEP

Key Index: 1

□ Use Passkey

Figure 7-21 *Encryption Dialog Box*

Table 7-10 *Encryption Options*

Encryption	Description
Open	Select *Open* (the default) when no data packet encryption is needed over the network. Selecting this option provides no security for data transmitting over the network.
40-Bit WEP	Select 40-Bit WEP to use 40-bit key length WEP encryption. WEP keys are manually entered in the edit boxes. Only the required number of edit boxes for a key length is displayed (10 Hex digit value for 40-bit keys). Use the *Key Index* drop-down list to configure the four WEP keys. The adapter uses the selected key. Note: The default Hex digit keys are visible any time they are used. As a security precaution after setting the key values for the network, the digits are replaced with asterisks * in the encryption key fields. If the associated AP uses an optional passkey, the active adapter WLAN profile must use one as well. The passkey is a plain text representation of the WEP keys displayed in the encryption dialog box. The passkey provides an easy way to enter WEP key data without having to remember the entire 40-bit (10 character) Hex digit string.
128-Bit WEP	Select 128-Bit WEP to use 128-bit key length WEP encryption. WEP keys are manually entered in the edit boxes. Only the required number of edit boxes for a key length is displayed (26 Hex digit value for 128-bit keys). Use the *Key Index* drop-down list to configure the four WEP keys. The adapter uses the selected key. Note: The default Hex digit keys are visible any time they are used. As a security precaution after setting the key values for the network, the digits are replaced with asterisks * in the encryption key fields. If the associated AP uses an optional passkey, the active adapter WLAN profile must use one as well. The passkey is a plain text representation of the WEP keys displayed in the encryption dialog box. The passkey provides an easy way to enter WEP key data without having to remember the entire 128-bit (26 character) Hex digit string.
TKIP	Select this option to use Wireless Protected Access (WPA) via TKIP. Manually enter the shared keys in the passkey field. Tap **Next** to display the passkey dialog box. Enter an 8 to 63 character string.

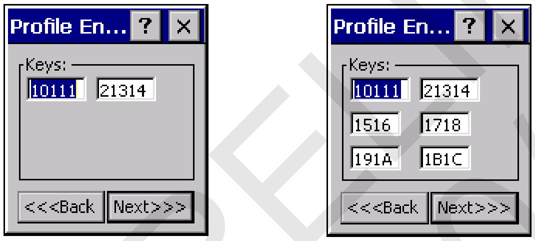
Table 7-11 *Encryption / Authentication Matrix*

	Encryption		
Authentication	**Open**	**WEP**	**TKIP**
None	Yes	Yes	Yes
EAP TLS	No	Yes	Yes
PEAP	No	Yes	Yes
LEAP	No	Yes	Yes
TTLS	No	Yes	Yes

Key Entry Page

If you select either *40-Bit WEP* or *128-Bit WEP* the wizard proceeds to the key entry dialog box unless the *Use Passkey* check box was selected in the *Encryption* dialog box (see *Figure 7-21 on page 7-15*). To enter the key information:

1. Enter the 40-bit or 128-bit keys into the fields.
2. Tap **Next**.



Keys: 10111 21314

Keys: 10111 21314 1516 1718 191A 1B1C

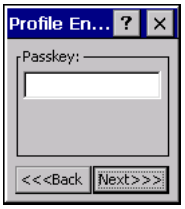
40-Bit WEP Keys Dialog Box 128-Bit WEP Keys Dialog Box

Figure 7-22 *40-Bit and 128-Bit WEP Keys Dialog Boxes*

Passkey Dialog

When you select *None* as an authentication and *WEP* as an encryption, you can choose to enter a passkey by checking the *Use PassKey* check box. The user is prompted to enter the passkey. For WEP, the *Use PassKey* checkbox is only available if the authentication is *None.*

When you select *None* as an authentication and *TKIP* as an encryption, you must enter a passkey. The user cannot enter a passkey if the encryption is *TKIP* and the authentication is anything other than *None*.



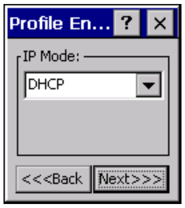
Passkey:

Figure 7-23 *Passkey Dialog Box*

Tap **Next**. The *IP Mode* dialog box displays.

IP Mode

Use the *IP Mode* dialog box to configure network address parameters: IP address, subnet, gateway, DNS, and WINS.



IP Mode: DHCP

Figure 7-24 *IP Config Tab (DHCP)*

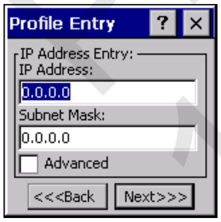
Table 7-12 *IP Mode Options*

Encryption	Description
DHCP	Select Dynamic Host Configuration Protocol (*DHCP*) from the *IP Mode* drop-down list to obtain a leased IP address and network configuration information from a remote server. DHCP is the default setting for the EDA profile. When DHCP is selected, the IP address fields are read-only.
Static	Select *Static* to manually assign the IP, subnet mask, default gateway, DNS, and WINS addresses the EDA profile uses.

Select either *DHCP* or *Static* from the drop-down list and tap **Next**. Selecting *Static IP* displays the *IP Address Entry* dialog box. Selecting *DHCP* displays the *Transmit Power* dialog box.

IP Address Entry

Use the *IP Address Entry* dialog box to enter the IP address and subnet information.



IP Address Entry:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

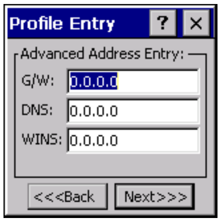
□ Advanced

Figure 7-25 *Static IP Address Entry Dialog Box*

Table 7-13 *Static IP Address Entry Fields*

Field	Description
IP Address	The Internet is a collection of networks with users that communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address (Internet Protocol address). Each node on the IP network must be assigned a unique IP address that is made up of a network identifier and a host identifier. Enter the IP address as a dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.
Subnet Mask	Most TCP/IP networks use subnets to manage routed IP addresses. Dividing an organization's network into subnets allows it to connect to the Internet with a single shared network address, for example, 255.255.255.0.

Select the *Advanced* check box, then tap **NEXT** to display the *Advanced Address Entry* dialog box. Enter the Gateway, DNS, and WINS address. Tap **NEXT** without selecting the *Advanced* check box to display the *Transmit Power* dialog box.



Advanced Address Entry:

G/W: 0.0.0.0

DNS: 0.0.0.0

WINS: 0.0.0.0

Figure 7-26 *Advanced Address Entry Dialog Box*

The IP information entered in the profile is only used if you selected the *Enable IP Mgmt* check box in the *Options - System Options* dialog box (*System Options on page 7-36*). If you didn't select this, the IP information in the profile is ignored and the IP information entered in the Microsoft interface applies.

Table 7-14 *IP Config Advanced Address Entry Fields*

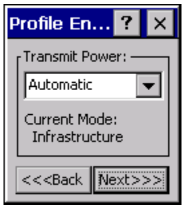
Field	Description
G/W	The default gateway forwards IP packets to and from a remote destination.
DNS	The Domain Name System (DNS) is a distributed Internet directory service. DNS translates domain names and IP addresses, and controls Internet email delivery. Most Internet services require DNS to operate properly. If DNS is not configured, Web sites cannot be located and/or email delivery fails.
WINS	WINS is a Microsoft® Net BIOS name server. WINS eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.

Tap **Next**. The *Transmit Power* dialog box displays.

Transmit Power

The *Transmit Power* drop-down list contains different options for Ad-Hoc and Infrastructure mode. Automatic (i.e., use the current AP settings) and Power Plus (use higher than the current AP settings) are available for *Infrastructure* mode.

Adjusting the radio transmission power level enables the user to expand or confine the transmission area with respect to other wireless devices that could be operating nearby. Reducing coverage in high traffic areas improves transmission quality by reducing the amount of interference in that coverage area.



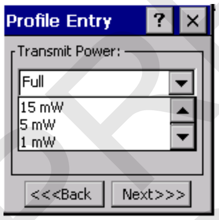
Transmit Power: Automatic

Current Mode: Infrastructure

Figure 7-27 *Transmit Power Dialog Box (Infrastructure Mode)*

Table 7-15 *Transmit Power Dialog Box (Infrastructure Mode)*

Field	Description
Automatic	Select *Automatic* (the default) to use the AP power level.
Power Plus	Select *Power Plus* to set the EDA transmission power one level higher than the level set for the AP.



Transmit Power: Full

Figure 7-28 *Transmit Power Dialog Box (Ad-Hoc Mode)*

Table 7-16 *Power Transmit Options (Ad-Hoc Mode)*

Field	Description
Full	Select *Full* power for the highest transmission power level. Select *Full* power when operating in highly reflective environments and areas where other devices could be operating nearby, or when attempting to communicate with devices at the outer edge of a coverage area.
30 mW	Select *30 mW* to set the transmit power level to 30 mW.

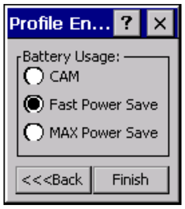
Table 7-16 *Power Transmit Options (Ad-Hoc Mode) (Continued)*

Field	Description
15 mW	Select *15 mW* to set the transmit power level to 15 mW.
5 mW	Select *5 mW* to set the transmit power level to 5 mW.
1 mW	Select *1 mW* for the lowest transmission power level. Use this level when communicating with other devices in very close proximity, or in instances where you expect little or no radio interference from other devices.

Tap **Next** to display the *Battery Usage* dialog box.

Battery Usage

Use the *Battery Usage* dialog box to select power consumption of the wireless LAN. There are three settings available: CAM, Fast Power Save, and MAX Power Save. Battery usage cannot be configured in Ad-Hoc profiles.



Battery Usage:
○ CAM
● Fast Power Save
○ MAX Power Save

Figure 7-29 *Battery Usage Dialog Box*

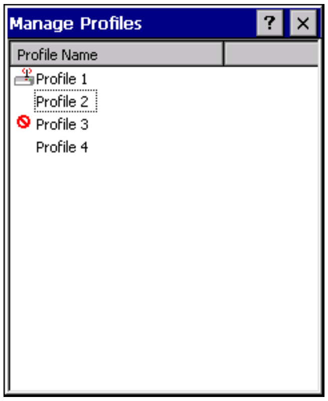
✓ ***NOTE*** Power consumption is also related to the transmit power settings.

Table 7-17 *Battery Usage Options*

Field	Description
CAM	Continuous Aware Mode (*CAM*) provides the best network performance, but yields the shortest battery life.
Fast Power Save	*Fast Power Save* (the default) performs in the middle of CAM and MAX Power Save with respect to network performance and battery life.
MAX Power Save	*Max Power Save* yields the longest battery life while potentially reducing network performance. In networks with minimal latency, Max Power Save performs as well as Fast Power Save, but with increased battery conservation.

Manage Profiles Application

The *Manage Profiles* window provides a list of user-configured wireless profiles. Define up to 32 profiles at any one time. To open the *Manage Profiles* window, tap the *Signal Strength* icon - *Manage Profiles*.



Manage Profiles

Profile Name

Profile 1

Profile 2

Profile 3

Profile 4

Figure 7-30 *Manage Profiles Window*

Icons next to each profile identify the profile's current state.

Table 7-18 *Profile Icons*

Icon	Description
No Icon	Profile is not selected, but enabled.
🚫	Profile is disabled.
⊗	Profile is cancelled. A cancelled profile is disabled until a connect or login function is performed through the configuration editor.
📡	Profile is in use and describes an infrastructure profile not using encryption.
🔑📡	Profile is in use and describes an infrastructure profile using encryption.
🖥	Profile is in use and describes an ad-hoc profile not using encryption.
🖥🔑	Profile is in use and describes an ad-hoc profile using encryption.
⚠	Profile is not valid in the device current operating regulatory domain.

The profiles are listed in priority order for use by the automatic roaming feature. Change the order by moving profiles up or down. To edit existing profiles, tap and hold one in the list and select an option from the menu to connect, edit, disable (enable), or delete the profile. (Note that the *Disable* menu item changes to *Enable* if the profile is already disabled.)

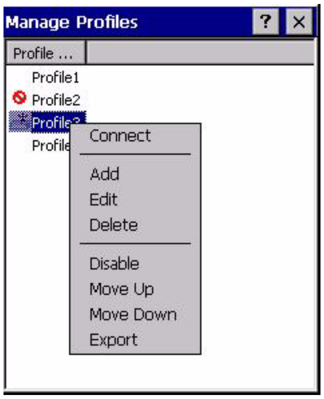


Figure 7-31 *Manage Profiles Context Menu*

Changing Profiles

A completed profile is a set of configuration settings that can be used in different locations to connect to a wireless network. Create different profiles to have pre-defined operating parameters available for use in various network environments. When the *WLAN Profile*s window displays, existing profiles appear in the list.

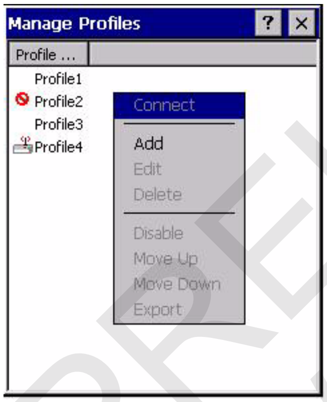


Figure 7-32 *Manage Profiles*

Tap and hold a profile and select *Connect* from the pop-up menu to set this as the active profile. Once selected, the EDA uses the authentication, encryption, ESSID, IP Config, and power consumption settings configured for that profile.

Editing a Profile

Tap and hold a profile and select *Edit* from the pop-up menu to display the *Profile Wizard* where you can set the ESSID and operating mode for the profile. Use the *Profile Wizard* to edit the profile power consumption and security parameters*. See Profile Editor Wizard on page 7-4*.

Creating a New Profile

To create new profiles from the *Manage Profiles* window, tap-and-hold anywhere in this window.

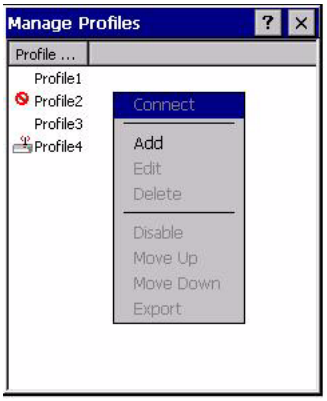


Figure 7-33 *Manage Profiles - Add*

Select *Add* to display the *Profile Wizard* wherein you can set the profile name and ESSID. Set security, network address information, and power consumption level for the new profile.

Deleting a Profile

To delete a profile from the list, tap and hold and select *Delete* from the pop-up menu. A confirmation dialog box appears.

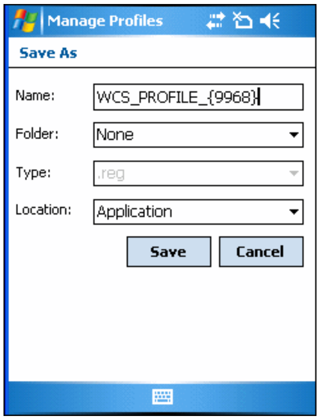
Ordering Profiles

Tap and hold a profile from the list and select *Move Up* or *Move Down* to order the profile. If the current profile association is lost, the EDA attempts to associate with the first profile in the list, then the next, until it achieves a new association.

✓ ***NOTE*** Profile Roaming must be enabled.

Export a Profile

To export a profile to a registry file, tap and hold a profile from the list and select *Export* from the pop-up menu. The *Save As* dialog box displays with the *Application* folder and a default name of WCS_PROFILE{*profile GUID*}.reg (Globally Unique Identifier).



Name: WCS_PROFILE_{9968}

Folder: None

Type: .reg

Location: Application

Figure 7-34 *Save As Dialog Box*

If required, change the name in the *Name* field and tap **Save**. A confirmation dialog box appears after the export completes.

Wireless Status Application

To open the *Wireless Status* window, tap the *Signal Strength* icon - *Wireless Status*. The *Wireless Status* window displays information about the wireless connection.

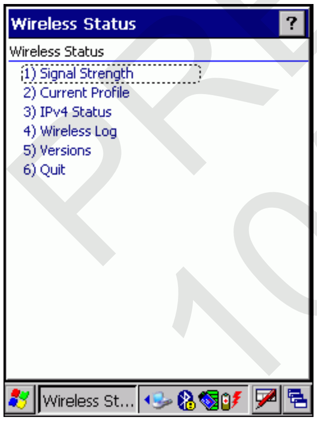


Figure 7-35 *Wireless Status Window*

The *Wireless Status* window contains the following options. Tap the option to display the option window.

- Signal Strength - provides information about the connection status of the current wireless profile.
- Current Profile - displays basic information about the current profile and connection settings.
- IPv4 Status - displays the current IP address, subnet, and other IP related information assigned to the EDA.

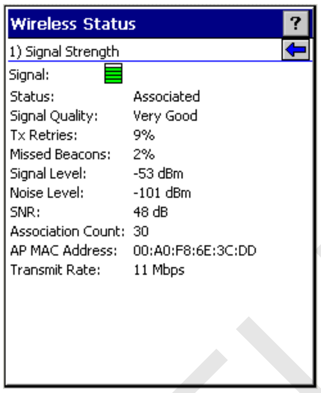
- Wireless Log - displays a log of important recent activity, such as authentication, association, and DHCP renewal completion, in time order.
- Versions - displays software, firmware, and hardware version numbers.
- Quit - exits the *Wireless Status* window.

Option windows contain a back button ⬅ to return to the main *Wireless Status* window.

Signal Strength Window

The *Signal Strength* window provides information about the connection status of the current wireless profile including signal quality, missed beacons, and transmit retry statistics. The BSSID address (shown as *AP MAC Address*) displays the AP currently associated with the connection. In Ad-Hoc mode, the AP MAC Address shows the BSSID of the Ad-Hoc network. Information in this window updates every 2 seconds.

To open the *Signal Status* window, tap *Signal Strength* in the *Wireless Status* window.



Signal:	🟩
Status:	Associated
Signal Quality:	Very Good
Tx Retries:	9%
Missed Beacons:	2%
Signal Level:	-53 dBm
Noise Level:	-101 dBm
SNR:	48 dB
Association Count:	30
AP MAC Address:	00:A0:F8:6E:3C:DD
Transmit Rate:	11 Mbps

Figure 7-36 *Signal Strength Window*

After viewing the *Signal Strength* window, tap the back button to return to the *Wireless Status* window.

Table 7-19 *Signal Strength Status*

Field	Description
Signal	Displays the Relative Signal Strength Indicator (RSSI) of the signal transmitted between the AP and EDA. As long as the Signal Quality icon is green the AP association is not jeopardized. If the icon is red (poor signal), an association with a different AP could be warranted to improve the signal. The signal strength icon changes depending on the signal strength. 🟩 Excellent Signal 🟩 Very Good Signal 🟨 Good Signal 🟨 Fair Signal ▭ Poor Signal ☒ Out of Range (no signal) ☒ The radio card is off or there is a problem communicating with the radio card.
Status	Indicates if the EDA is associated with the AP.
Signal Quality	Displays a text format of the Signal icon.

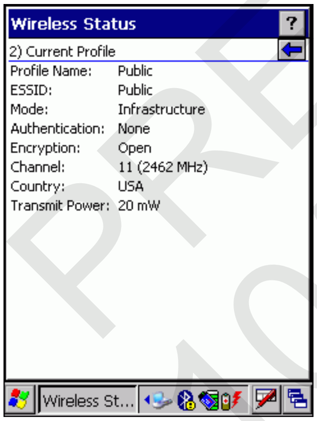
Table 7-19 *Signal Strength Status (Continued)*

Field	Description
Tx Retries	Displays a percentage of the number of data packets the EDA retransmits. The fewer transmit retries, the more efficient the wireless network is.
Missed Beacons	Displays a percentage of the amount of beacons the EDA missed. The fewer transmit retries, the more efficient the wireless network is. Beacons are uniform system packets broadcast by the AP to keep the network synchronized.
Signal Level	The AP signal level in decibels per milliwatt (dBm).
Noise Level	The background interference (noise) level in decibels per milliwatt (dBm).
SNR	The access point/EDA Signal to Noise Ratio (SNR) of signal strength to noise (interference) in decibels per milliwatt (dBm).
Association Count	Displays the number of APs the EDA connects to while roaming.
AP MAC Address	Displays the MAC address of the AP to which the EDA is connected.
Transmit Rate	Displays the current rate of the data transmission.

Current Profile Window

The *Current Profile* window displays basic information about the current profile and connection settings. This window updates every two seconds.

To open the *Current Profile* window, tap *Current Profile* in the *Wireless Status* window.



Wireless Status

2) Current Profile

Profile Name:	Public
ESSID:	Public
Mode:	Infrastructure
Authentication:	None
Encryption:	Open
Channel:	11 (2462 MHz)
Country:	USA
Transmit Power:	20 mW

Figure 7-37 *Current Profile Window*

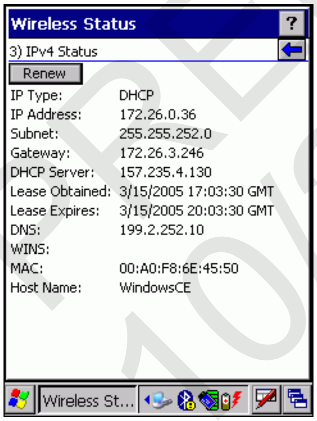
Table 7-20 *Current Profile Window*

Field	Description
Profile Name	Displays the current profile name the EDA uses to communicate with the AP.
ESSID	Displays the current profile ESSID name.
Mode	Displays the current profile mode, either Infrastructure or Ad-Hoc.
Authentication	Displays the current profile’s authentication type.
Encryption	Displays the current profile’s encryption type.
Channel	Displays the current profile’s channel setting.
Country	Displays the current profile’s country setting.
Transmit Power	Displays the radio transmission power level.

IPv4 Status Window

The *IPv4 Status* window displays the current IP address, subnet, and other IP related information assigned to the EDA. It also allows renewing the address if the profile is using DHCP to obtain the IP information. Tap **Renew** to initiate a full DHCP discover. The *IPv4 Status* window updates automatically when the IP address changes.

To open the *IPv4 Status* window, tap *IPv4 Status* in the *Wireless Status* window.



IP Type:	DHCP
IP Address:	172.26.0.36
Subnet:	255.255.252.0
Gateway:	172.26.3.246
DHCP Server:	157.235.4.130
Lease Obtained:	3/15/2005 17:03:30 GMT
Lease Expires:	3/15/2005 20:03:30 GMT
DNS:	199.2.252.10
WINS:	
MAC:	00:A0:F8:6E:45:50
Host Name:	WindowsCE

Figure 7-38 *IPv4 Status Window*

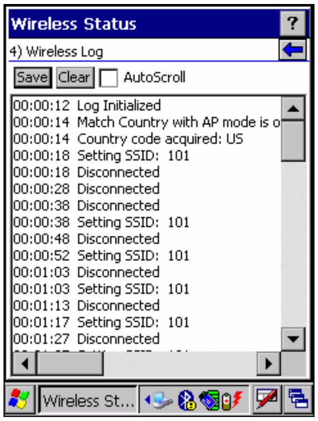
Table 7-21 *IPv4 Status Fields*

Field	Description
IP Type	Displays the IP type for the current profile: *DHCP* or *Static*. If the IP type is DHCP, leased IP address and network address data appear for the EDA. If the IP type is Static, the values displayed were input manually in the *IP Config* tab on page 7-17.
IP Address	Displays the EDA’s IP address. The Internet is a collection of networks with users that communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address. Each node on the IP network must be assigned a unique IP address that is made up of a network identifier and a host identifier. The IP address as a dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.
Subnet	Displays the subnet address. Most TCP/IP networks use subnets to manage routed IP addresses. Dividing an organization's network into subnets allows it to connect to the Internet with a single shared network address, for example, 255.255.255.0.
Gateway	Displays the gateway address. A gateway forwards IP packets to and from a remote destination.
DCHP Server	The Domain Name System (DNS) is a distributed Internet directory service. DNS translates domain names and IP addresses, and controls Internet e-mail delivery. Most Internet services require DNS to operate properly. If DNS is not configured, Web sites cannot be located or e-mail delivery fails.
Lease Obtained	Displays the date that the IP address was obtained.
Lease Expires	Displays the date that the IP address expires and a new IP address is requested.
DNS	Displays the IP address of the DNS server.
WINS	WINS is a Microsoft Net BIOS name server. WINS eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.
MAC	An IEEE 48-bit address is assigned to the EDA at the factory to uniquely identify the adapter at the physical layer.
Host Name	Displays the name of the EDA.

Wireless Log Window

The *Wireless Log* window displays a log of recent activity, such as authentication, association, and DHCP renewal completion, in time order. Save the log to a file or clear the log (within this instance of the application only). The auto-scroll feature automatically scrolls down when new items are added to the log.

To open the *Wireless Log* window, tap *Wireless Log* in the *Wireless Status* window. The *Wireless Log* window displays.



```
00:00:12  Log Initialized
00:00:14  Match Country with AP mode is o
00:00:14  Country code acquired: US
00:00:18  Setting SSID:  101
00:00:18  Disconnected
00:00:28  Disconnected
00:00:38  Disconnected
00:00:38  Setting SSID:  101
00:00:48  Disconnected
00:00:52  Setting SSID:  101
00:01:03  Disconnected
00:01:03  Setting SSID:  101
00:01:13  Disconnected
00:01:17  Setting SSID:  101
00:01:27  Disconnected
```

Figure 7-39 *Wireless Log Window*

Saving a Log

To save a Wireless Log:

1. Tap the **Save** button. The *Save As* dialog box displays.
2. Navigate to the desired folder.
3. In the *Name* filed, enter a file name and then tap **OK**. A text file is saved in the selected folder.

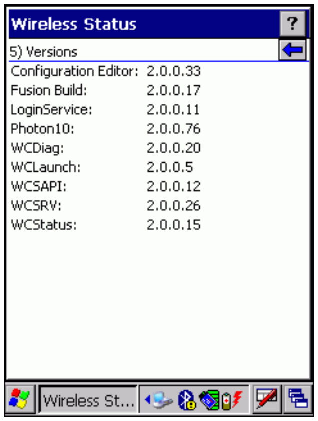
Clearing the Log

To clear the log, tap **Clear**.

Versions Window

The *Versions* window displays software, firmware, and hardware version numbers. This window only updates when it is displayed. There is no need to update constantly. The content of the window is determined at runtime, along with the actual hardware and software to display in the list. Executable paths of the software components on the list are defined in registry, so that the application can retrieve version information from the executable. “File not found” appears if the executable cannot be found at the specified path.

To open the *Versions* window, tap *Versions* in the *Wireless Status* window.



Configuration Editor:	2.0.0.33
Fusion Build:	2.0.0.17
LoginService:	2.0.0.11
Photon10:	2.0.0.76
WCDiag:	2.0.0.20
WCLaunch:	2.0.0.5
WCSAPI:	2.0.0.12
WCSRV:	2.0.0.26
WCStatus:	2.0.0.15

Figure 7-40 *Versions Window*

The window displays software version numbers for the following:

- Configuration Editor
- Fusion Build
- LoginService
- Photon1.0
- WCDiag
- WCLaunch
- WCSAPI
- WCSRV
- WCStatus.

Wireless Diagnostics Application

The *Wireless Diagnostics* application window provides links to perform ICMP Ping, Trace Routing, and Known APs. To open the *Wireless Diagnostics* window, tap the *Signal Strength* icon - *Wireless Diagnostics*.

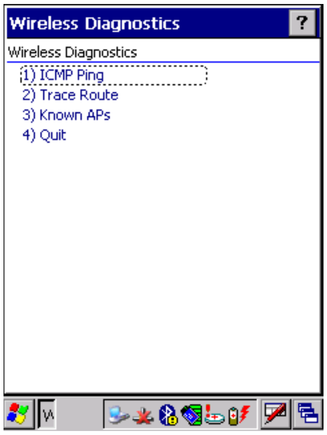


Figure 7-41 *Wireless Diagnostics Window*

The *Wireless Diagnostics* window contains the following options. Tap the option to display the option window.

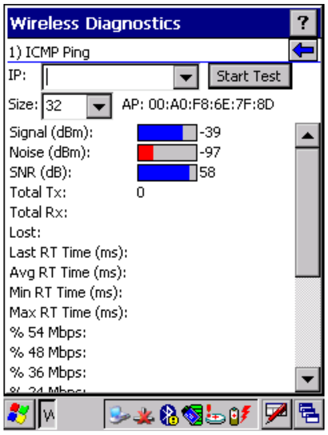
- ICMP Ping - tests the wireless network connection.
- Trace Route - tests a connection at the network layer between the EDA and any place on the network.
- Known APs - displays the APs in range using the same ESSID as the EDA.
- Quit - Exits the *Wireless Diagnostics* window.

Option windows contain a back button ⬅ to return to the *Wireless Diagnostics* window.

ICMP Ping Window

The *ICMP Ping* window allows testing a connection at the network layer (part of the IP protocol) between the EDA and an AP. Ping tests only stop when you tap the **Stop Test** button, close the *Wireless Diagnostics* application, or if the EDA switches between infrastructure and ad-hoc modes.

To open the *ICMP Ping* window, tap the *ICMP Ping* in the *Wireless Diagnostics* window.



1) ICMP Ping
IP:
Size: 32 AP: 00:A0:F8:6E:7F:8D
Signal (dBm): -39
Noise (dBm): -97
SNR (dB): 58
Total Tx: 0
Total Rx:
Lost:
Last RT Time (ms):
Avg RT Time (ms):
Min RT Time (ms):
Max RT Time (ms):
% 54 Mbps:
% 48 Mbps:
% 36 Mbps:

Figure 7-42 *ICMP Ping Window*

To perform an ICMP ping:

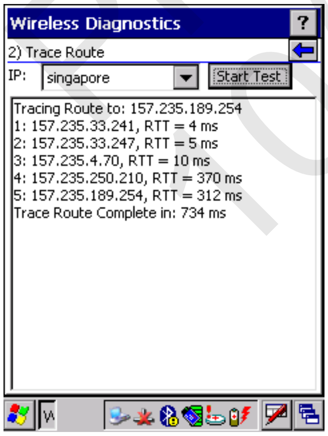
1. In the *IP* field, enter an IP address or select an IP address from the drop-down list.
2. From the *Size* drop-down list, select a size value.
3. Tap **Start Test**. The ICMP Ping test starts. Information of the ping test displays in the appropriate fields.

Trace Route Window

Trace Route traces a packet from a computer to a host, showing how many hops the packet requires to reach the host and how long each hop takes. The *Trace Route* utility identifies where the longest delays occur.

The *Trace Route* window allows testing a connection at the network layer (part of the IP protocol) between the EDA and any place on the network.

To open the *Trace Route* window, tap *Trace Route* in the *Wireless Diagnostics* window.



2) Trace Route
IP: singapore

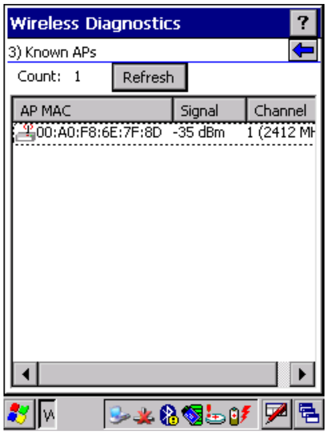
```
Tracing Route to: 157.235.189.254
1: 157.235.33.241, RTT = 4 ms
2: 157.235.33.247, RTT = 5 ms
3: 157.235.4.70, RTT = 10 ms
4: 157.235.250.210, RTT = 370 ms
5: 157.235.189.254, RTT = 312 ms
Trace Route Complete in: 734 ms
```

Figure 7-43 *Trace Route Window*

Enter an IP address or a DNS Name in the IP combo box, and tap **Start Test**. The IP combo box should match the information shown in the *ICMP Ping* window's IP combo box. When starting a test, the trace route attempts to find all routers between the EDA and the destination. The Round Trip Time (RTT) between the EDA and each router appears, along with the total test time. The total test time may be longer than all RTTs added together because it does not only include time on the network.

Known APs Window

The *Known APs* window displays the APs in range using the same ESSID as the EDA. This window is only available in *Infrastructure* mode. To open the *Known APs* window, tap *Known APs* in the *Wireless Diagnostics* window.



Wireless Diagnostics

3) Known APs

Count: 1 Refresh

AP MAC	Signal	Channel
00:A0:F8:6E:7F:8D	-35 dBm	1 (2412 MH

Figure 7-44 *Known APs Window*

See Table 7-22 for the definitions of the icons next to the AP.

Table 7-22 *Current Profile Window*

Icon	Description
M	The AP is the associated access point, and is set to mandatory.
	The AP is the associated access point, but is not set to mandatory.
M	The EDA is not associated to this AP, but the AP is set as mandatory.
	The EDA is not associated to this AP, and AP is not set as mandatory.

Tap and hold on an AP to display a pop-up menu with the following options: *Set Mandatory* and *Set Roaming*.

Select *Set Mandatory* to prohibit the EDA from associating with a different AP. The letter *M* displays on top of the icon. The EDA connects to the selected AP and never roams until:

- You select *Set Roaming*
- The EDA roams to a new profile
- The EDA suspends
- The EDA resets (warm or cold).

Select *Set Roaming* to allow the EDA to roam to any AP with a better signal. These settings are temporary and never saved to the registry.

Tap **Refresh** to update the list of the APs with the same ESSID. The highest signal strength value is 32.

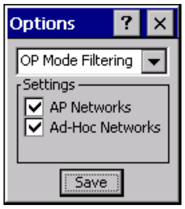
Options

Use the wireless *Option* dialog box to select one of the following operation options from the drop-down list:

- Operating Mode Filtering
- Regulatory
- Band Selection
- System Options
- Change Password
- Export.

Operating Mode Filtering

The *Operating Mode Filtering* options cause the Find WLANs application to filter the available networks found.



Settings

☑ AP Networks

☑ Ad-Hoc Networks

Figure 7-45 *OP Mode Filtering Dialog Box*

The *AP Networks* and *Ad-Hoc Networks* check boxes are selected by default.

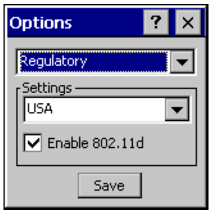
Table 7-23 *OP Mode Filtering Options*

Field	Description
AP Networks	Select the *AP Networks* check box to display available AP networks and their signal strength within the *Available WLAN Networks* (see *Find WLANs Application on page 7-3*). These are the APs available to the EDA profile for association. If this option was previously disabled, refresh the *Available WLAN Networks* window to display the AP networks available to the EDA.
AD-Hoc Networks	Select the *Ad-Hoc Networks* check box to display available peer (adapter) networks and their signal strength within the *Available WLAN Networks*. These are peer networks available to the EDA profile for association. If this option was previously disabled, refresh the *Available WLAN Networks* window to display the Ad Hoc networks available to the EDA.

Tap **Save** to save the settings or tap **X** to discard any changes.

Regulatory Options

Use the *Regulatory* settings to configure the country the EDA is in. Due to regulatory requirements (within a country) a EDA is only allowed to use certain channels.



Options

Regulatory

Settings: USA

☑ Enable 802.11d

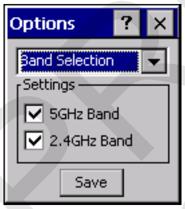
Figure 7-46 *Regulatory Options Dialog Box*

Table 7-24 *Regulatory Options*

Field	Description
Settings	Select the country from the drop-down list. To connect to a profile, the profile country must match this setting, or the AP country setting if you selected the *Enable 802.11d* check box.
Enable 802.11d	The WLAN adapter attempts to retrieve the country from APs. Profiles which use *Infrastructure* mode can only connect if the country set is the same as the AP country settings or if the profile country setting is *Allow Any Country*. All APs must be configured to transmit the country information.

Band Selection

The *Band Selection* settings identify the frequency bands to scan when finding WLANs. These values refer to the 802.11 standard networks.



Options

Band Selection

Settings

☑ 5GHz Band

☑ 2.4GHz Band

Figure 7-47 *Band Selection Dialog Box*

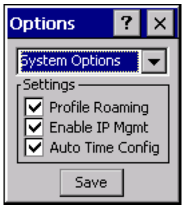
Table 7-25 *Band Selection Options*

Field	Description
5GHz Band	The *Find WLANs* application list includes all networks found in the 5 GHz band (802.11a).
2.4GHz Band	The *Find WLANs* application list includes all networks found in the 2.4 GHz band (802.11b and 802.11g).

Tap **Save** to save the settings or tap **X** to discard any changes.

System Options

Use *System Options* to set miscellaneous system setting.



☑ Profile Roaming
☑ Enable IP Mgmt
☑ Auto Time Config

Figure 7-48 *System Options Dialog Box*

Table 7-26 *System Options*

Field	Description
Profile Roaming	Configures the EDA to roam to the next available WLAN profile when it moves out of range of the current WLAN profile.
Enable IP Mgmt	Enables the Wireless Companion Services to handle IP address management. The Wireless Companion Service configures the IP based on what is configured in the network profile. Deselect this to manually configure the IP in the standard Windows IP window. Enabled by default.
Auto Time Config	Enables automatic update of the system time. Network association updates the device time based on the time set in the AP. This proprietary feature is only supported with Symbol infrastructure. Enabled by default.

Change Password

Use *Change Password* to require a password before editing a profile. This allows pre-configuring profiles and prevents users from changing the network settings. The user can use this feature to protect settings from a guest user. By default, the password is not set.

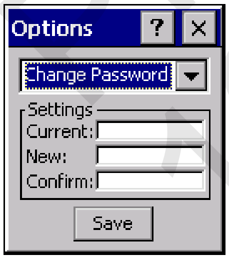


Figure 7-49 *Change Password Window*

To create a password for the first time, leave the *Current:* text box empty and enter the new password in the *New:* and *Confirm:* text boxes. Tap **Save**.

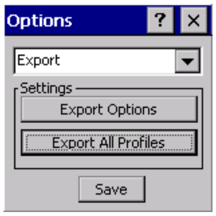
To change an existing password, enter the current password in the *Current:* text box and enter the new password in the *New:* and *Confirm:* text boxes. Tap **Save**.

To delete the password, enter the current password in the *Current:* text box and leave the *New*: and *Confirm:* text boxes empty. Tap **Save.**

✓ ***NOTE*** Passwords are case sensitive and can not exceed 10 characters.

Export

Use *Export* to export all profiles to a registry file, and to export the options to a registry file.



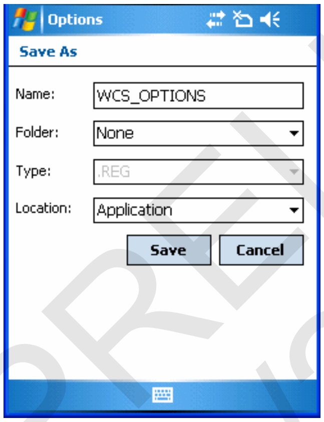
Options

Export

Figure 7-50 *Options - Export Dialog Box*

To export options:

1. Tap **Export Options**. The *Save As* dialog box displays.



Options

Save As

Name: WCS_OPTIONS

Folder: None

Type: .REG

Location: Application

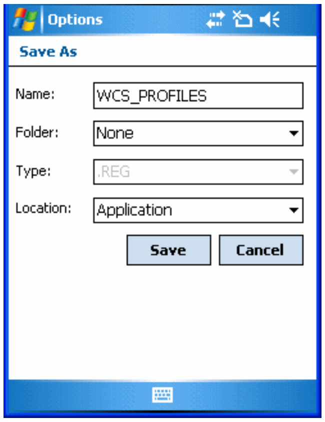
Figure 7-51 *Export Options Save As Dialog Box*

2. Enter a filename in the *Name*: field. The default filename is WCS_OPTIONS.REG.

3. Tap **Save**.

To export all profiles:

1. Tap **Export All Profiles**. The *Save As* dialog box displays.



Name: WCS_PROFILES
Folder: None
Type: .REG
Location: Application

Figure 7-52 *Export All Profiles Save As Dialog Box*

2. Enter a filename in the *Name*: field. The default filename is WCS_PROFILES.REG.
3. In the *Folder:* drop-down list, select the desired folder.
4. Tap **Save**.

Selecting **Export All Profiles** saves the current profile. This information is used to determine which profile to connect with after a warm boot or cold boot.

Cold Boot Persistence

Export options and profiles to provide cold boot persistence. Save the exported registry files in the *Application* folder to use them on a cold boot and restore previous profile and option settings.

Currently, only server certificates can be saved for cold boot persistence. To save server certificates for cold boot persistence, save the certificate files in the folder *Application\Certs* to install the certificates automatically on a cold boot.

NOTE User certificates cannot be saved for cold boot persistence at this time.

Registry Settings

Use a registry key to modify some of the parameters. The registry path is:

HKLM\SOFTWARE\Symbol Technologies, Inc.\Configuration Editor

Table 7-27 *Registry Parameter Settings*

Key	Type	Default	Description
CertificateDirectory	REG_SZ	\\Windows	The default directory to find certificates.
EncryptionMask	REG_DWORD	0x0000001F	Defines the supported encryption types. This is a bitwise mask with each bit corresponding to an encryption type. 1 = Type is supported 0 = Type is not supported Bit Number Encryption Type 0 None 1 40-Bit WEP 2 128-Bit WEP 3 TKIP
MenuShortCut	REG_SZ	Alt-M	Describes the key combination to use for menu selection. Tap-and-hold or use a key sequence to display menus. This value can be a system key sequence (i.e., preceded with ALT) or a single key which triggers a pop-up menu when the appropriate dialog is visible.
RefreshTime	REG_DWORD	4000	This registry key defines the number of milliseconds between refreshes of the *Manage Profiles* window.

Log On/Off Application

When the user launches the Log On/Off application, the EDA may be in two states; the user may be logged onto the EDA by already entering credentials through the login box, or there are no user logged on. Each of these states have a separate set of use cases and a different look to the dialog box.

User Already Logged In

If already logged into the EDA, the user can launch the login dialog box for the following reasons:

- Connect to and re-enable a cancelled profile. To do this:
  - Launch the password dialog.
  - Select the cancelled profile from the profile list.
  - Login to the profile.

NOTE Re-enable cancelled profiles using the Profile Editor Wizard and choosing to connect to the cancelled profile. Cancelled profiles are also re-enabled when a new user logs on.

- Log off the EDA to prevent another user from accessing the current users network privileges.
- Switch EDA users to quickly logoff the EDA and allow another user to log into the EDA.

No User Logged In

If no user is logged into the EDA, launch the login dialog box and log in to access user profiles.

The *Login* dialog box varies if it is:

- Launched by WCS, because the service is connecting to a new profile that needs credentials.
- Launched by WCS, because the service is trying to verify the credentials due to credential caching rules.
- Launched by a user, when a user is logged in.
- Launched by a user, when no user is logged in.

Device Username Field

The device username is a high level username used to link different network credentials to the same person as explained above. The Device Username field is only writable when there is no user logged on. Otherwise it is static text. The Device Username has a maximum length defined in the WCSAPI.

Table 7-28 *Log On/Off Options*

Field	Description
Wireless Profile Field	When launching the login application, the Wireless Profile field has available all the wireless profiles that require credentials. This includes profiles that use EAP TLS, PEAP, LEAP, and EAP-TTLS.
Profile Status Icon	The profile status icon (next to the profile name) shows one of the following states: The selected profile is cancelled. The selected profile is enabled but is not the current profile. The profile is the current profile (always the case for WCS Launched).
Network Username and Password Fields	The Network Username and Network Password fields are used as credentials for the profile selected in the Wireless Profile field. Currently these fields are limited to 159 characters.
Mask Password Checkbox	The *Mask Password* checkbox determines whether the password field is masked (i.e., displays only the '*' character) or unmasked (i.e., displays the entered text). Check the box to unmask the password. Uncheck the box to mask the password (the default).
Status Field	The status field displays status that is important to the login dialog. If the user opens the dialog and needs to prompt for credentials for a particular profile at this time, it can use the status field to let the user know that the network is held up by the password dialog being open.

Tapping **OK** sends the credentials though WCS API. If there are no credentials entered, a dialog box displays informing the user which field was not entered.

The **Log Off** button only displays when a user is already logged on. When the **Log Off** button is tapped, the user is prompted with three options: Log Off, Switch Users, and Cancel. Switching users logs off the current user and re-initialize the login dialog box to be displayed for when there is no user logged on. Logging off logs off the current user and close the login dialog box. Tapping **Cancel** closes the Log Off dialog box and the Login dialog box displays.

When the user is logged off, the EDA only roams to profiles that do not require credentials or to profiles that were created with the credentials entered into the profile

The **Cancel** button closes the dialog without logging into the network. If the login dialog was launched by the wCS and not by the user, tapping **Cancel** first causes a message box to display a warning that the cancel disables the current profile. If the user still chooses to cancel the login at this point, the profile is cancelled.

Once a profile is cancelled, the profile is suppressed until a user actively re-enables it or a new user logs onto the EDA.